COURSE DESCRIPTION CARD - SYLLABUS

Course name
Introduction to Open-Source Intelligence (OSINT) [S1Cybez1>WdBW]

Course

Field of study
Cybersecurity

Year/Semester
3/5

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
16

Laboratory classes
0

Other
0

Tutorials
0

Projects/seminars
30

Number of credit points

3,00

Coordinators

dr inż. Michał Weissenberg
michal.weissenberg@put.poznan.pl

dr hab. inż. Sławomir Hanczewski
slawomir.hanczewski@put.poznan.pl

Lecturers

Prerequisites

• Basic computer operation and internet usage skills. • Ability to use web browsers and basic information search tools. • Basic knowledge of data protection and online privacy.

Course objective

The goal of this course is to familiarize students with the fundamental principles, methods, and tools used in open-source intelligence (OSINT). Students will learn to ethically and legally identify, collect, analyze, and interpret publicly available data, as well as explore practical OSINT applications in cybersecurity. An additional objective of the course is to develop ethical and legal awareness in handling information.

Course-related learning outcomes

Knowledge:
• Knows the basic OSINT techniques and tools. [K1_W06]
• Understands the significance of open-source data in data analysis and threat detection. [K1_W20]

• Understands the legal and ethical aspects of conducting open-source intelligence. [K1_W21]

Skills:
• Is able to search for and analyze information from open sources. [K1_U01]
• Can apply selected OSINT tools in practical projects. [K1_U02]
• Can document analysis results in a clear and professional manner. [K1_U04]

Social competences:
• Understands the necessity of ethical conduct when using information from open sources. [K1_K05]
• Is aware of the risks associated with the improper use of data. [K1_K02]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

• A written test verifying knowledge in the field of open-source intelligence and familiarity with OSINT tools and techniques. Open and closed questions.
• A team project: case analysis using selected OSINT tools.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

Programme content

This course introduces students to the use of open-source intelligence (OSINT) techniques for acquiring and analyzing information from publicly available sources. It covers fundamental tools and methods for exploring the informational environment, identifying threats, and supporting decision-making processes in the field of cybersecurity.

Course topics

• Fundamentals of OSINT (Open-Source Intelligence): Definitions, objectives, ethics, and legal regulations.
• OSINT Information Sources: Analysis of data from social media, public registries, databases, and online resources.
• OSINT Techniques and Tools: Overview of popular tools such as Maltego, SpiderFoot, and Shodan.
• OSINT Data Analysis: Methods of processing and visualizing collected data.
• OSINT Applications in Cybersecurity: Threat detection, environment monitoring, and incident analysis.
• Legal and Ethical Aspects of OSINT: Legal and moral boundaries in the use of open-source data.

Teaching methods

• Lectures online with multimedia presentations.
• Team projects: practical use of OSINT tools in defined cases.

Bibliography

Basic:
• Justin Seitz, Automating OSINT with Python, No Starch Press, 2021.
• Michael Bazzell, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 2022.

Additional:
• Open-source tools and documentation, e.g., Shodan, Maltego, SpiderFoot.
• Harleen Kaur, M. OSINT for Hackers and Investigators: A Primer on Open Source Intelligence, Apress, 2020.

Breakdown of average student's workload

	Hours	ECTS
Total workload	90	3,00
Classes requiring direct contact with the teacher	46	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	44	1,50